UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,094	10/10/2001	Martin Langhammer	ALTRP062/A603	7694

51501 7590 03/23/2006

BEYER WEAVER & THOMAS, LLP
ATTN: ALTERA
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/975,094	LANGHAMMER ET AL.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 October 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 October 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) ~~Paper No(s)/Mail Date _____~~. P, C
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-50 are pending in the instant application and have been examined.

Information Disclosure Statement

2. The information disclosure statement filed 10-07-2002 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. Copies of all non-patent literature have become separated from or are missing from the IDS and, consequently, cannot be considered. The Applicant will unfortunately have to resubmit the non-Patent documents from the IDS if consideration of such is desired.

Oath/Declaration

3. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:
It was not executed in accordance with either 37 CFR 1.66 or 1.68.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 14-18, 23, 32, 33, 38, and 46-48 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Albrecht et al. US 5,835,594.

As for claims 1 and 38, Albrecht teaches a method for controlling use of configuration data (abstract: write data, fig. 7: element 306: write data, col. 4 lines 18-21) comprising: programming a configurable device using the configuration data provided by a secure device (col. 3 lines 32-43: "...creation of an electronic signature and associating it with write data..." This reads on configuration data created by a secure device, fig. 7: element 306: "write data", col. 4 lines 18-21: col. 2 lines 54-55: BIOS updates reads on configuration data), the programmed configurable device comprising: disabled user logic (col. 4 lines 25-30: the FLASH memory is write-disabled); and a comparator (fig. 2 element 120: Comparison Function); generating a configurable device authorization code (col. 2 lines 60-67: a reference digest of the configuration data is generated and signed. The digest is later used for authorizing the writing of configuration data to FLASH memory: this reads on an authorization code); transmitting the configurable device authorization code to the comparator (col. 2 lines 44-49, col. 3 lines 1-8); generating a secure device authorization code (col. 3 lines 1-8: a new copy of the reference digest is calculated); transmitting the secure device authorization code to the comparator (col. 3 lines 1-8); comparing the configurable device authorization code and the secure device authorization code (col. 3 lines 6-15);

and enabling the user logic if the configurable device authorization code and the secure device authorization code are identical (col. 3 lines 6-15: If the decrypted reference digest and the newly calculated reference digest match, then the FLASH memory is write-enabled).

As for claims 14-17, Albrecht teaches a method for controlling use of configuration data (abstract: write data, fig. 7: element 306: write data, col. 4 lines 18-21) comprising: programming a configurable device using the configuration data provided by a secure device (col. 3 lines 32-43: "...creation of an electronic signature and associating it with write data..." This reads on configuration data created by a secure device, fig. 7: element 306: "write data", col. 4 lines 18-21: col. 2 lines 54-55: BIOS updates reads on configuration data), comprising: programming a configurable device using the configuration data provided by a secure device (col. 2 lines 51-59: the "write data" is provided with an electronic signature, this reads on being provided by a secure device. The "write data" may comprise such data as BIOS updates to FLASH memory: This reads on programming a configurable device), the programmed configurable device comprising: disabled user logic (col. 4 lines 25-30: the FLASH memory is write disabled); a decryptor (fig. 4 element 268: BIOS: Decryption, col. 3 lines 3-4: "...secured complementary decryption function..."); a configurable device sequence generator (col. 3 lines 1-3: "...a secured corresponding copy of [the] message digest function generates a new digest...": This reads on a sequence generator in the configurable device); and a comparator (fig. 2 element 120: "Comparison Function");

generating a configurable device authorization code using the configurable device sequence generator (col. 2 lines 60-67: a reference digest of the configuration data is generated and signed. The digest is later used for authorizing the writing of configuration data to FLASH memory: this reads on an authorization code); transmitting the configurable device authorization code to the comparator (col. 3 lines 6-9); generating a first sequence in a secure device sequence generator in the secure device (col. 2 lines 43-51: a reference digest of the write data is calculated and signed, the reference digest is later used in an authorization function); encrypting the first sequence in an encryptor in the secure device to generate a second sequence (fig. 1 element 108: the reference digest is encrypted in the secure device, col. 2 lines 43-51, the reference digest is signed, i.e., encrypted under a private key); transmitting the second sequence to the decryptor (col. 3 lines 1-5, fig. 2 element 116: Decryption Function: the configurable device decrypts the signed reference digest received from the secure device) ; decrypting the second sequence to generate a third sequence (col. 3 lines 1-5, fig. 2 element 116: Decryption Function: the configurable device decrypts the signed reference digest received from the secure device); transmitting the third sequence as a secure device authorization code to the comparator (fig. 2 element 120: Comparison Function, col. 3 lines 6-9); comparing the secure device authorization code and the configurable device authorization code (col. 3 lines 6-9: the decrypted reference digest and the newly calculated reference digest are compared); and enabling the user logic if the configurable device authorization code and the secure device authorization code are

identical (col. 3 lines 12-14: A secure write function is enabled in the configurable device if the comparison is successful).

As for claim 18, Albrecht teaches the system of Claim 17, and the additional steps wherein: the configurable device generator comprises a sequence generator in the configurable device (col. 3 lines 1-3: the configurable device generates a new copy of the reference digest which reads on a sequence generator); and the secure device generator comprises: a sequence generator in the secure device (col. 2 lines 45-51: the secure device generates a reference digest of the write data: this reads on a sequence generator); an encryptor coupled to the secure device sequence generator and configured to encrypt a first sequence generated by the secure device sequence generator to generate a second sequence (col. 2 lines 47-49: the secure device "signs" the reference digest by encrypting it under its private key); and a decryptor in the configurable device (col. 3 lines 3-7: the configurable device decrypts the signed reference digest received from the secure device), the decryptor coupled to the encryptor and configured to decrypt the second sequence (col. 3 lines 3-7: the configurable device decrypts the signed reference digest received from the secure device) to generate a third sequence and to transmit the third sequence as the secure device authorization code to the first input of the comparator (col. 3 lines 3-6: "comparison function").

As for claim 23, Albrecht teaches the system of claim 17, and the additional steps wherein: the configurable device authorization code generator comprises a sequence generator in the configurable device (col. 3 lines 1-3: the configurable device generates a new reference digest, this reads on a sequence generator); and the secure device authorization code generator comprises a sequence generator in the secure device (col. 2 lines 51-59: a reference digest is generated in the secure device).

As for claim 32, Albrecht teaches the system of Claim 17, and the additional steps wherein: the secure device authorization code generator comprises a sequence generator in the secure device configured to generate a first sequence as the secure device authorization code (col. 2 lines 51-59); and the configurable device authorization code generator comprises: an encryptor in the secure device, the encryptor configured to receive and encrypt the first sequence to generate a second sequence (col. 2 lines 51-59: the secure device generates a reference digest and then encrypts it under a private key before sending it to the configurable device); and a decryptor in the configurable device, the decryptor configured to receive and decrypt the second sequence to generate a third sequence (col. 3 lines 3-7) and to transmit the third sequence as the configurable device authorization code to the comparator (col. 3 lines 3-7).

As for claim 33, Albrecht et al. teaches A system for controlling use of configuration data (abstract: write data, fig. 7: element 306: write data, col. 4 lines 18-

21) comprising: a secure device (col. 3 lines 32-43) comprising: a secure device sequence generator configured to generate a first sequence (col. 2 lines 60-67: The secure device calculates a reference digest of the write data, reading on a first sequence); and an encryptor configured to receive and encrypt the first sequence to generate a second sequence (col. 2 lines 60-67: The secure device encrypts the reference digest under a private key to form a signed digest, reading on a second sequence); and a configurable device comprising: disabled user logic (col. 4 lines 28-30); a decryptor configured to receive and decrypt the second sequence to generate a third sequence (fig. 2 element 116, col. 3 lines 3-6: The configurable device decrypts the signed reference digest using a public key corresponding to the private key: reading on the generation of a third sequence); a configurable device sequence generator configured to generate a fourth sequence (col. 3 lines 1-6: The configurable device generates a new reference digest using the write data) ; a comparator configured to receive and compare the third sequence and the fourth sequence (col. 3 lines 8-16: the decrypted digest and the new digest generated in the configurable device are sent to a comparator, fig. 2 element 120: Comparison Function); and means connected to the comparator and the user logic for enabling the user logic if the third and fourth sequences are identical (col. 3 lines 8-16).

As for claims 46-48, the claims are directed towards the apparatus that carries out the method set forth in claim 1 and contain substantially the same limitations. Therefore the claims are rejected on the same basis as is claim 1.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 28-31, 43, 49, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albrecht et al. US 5,835,594, and Shona, US 5,799,085.

As for claim 43, Albrecht teaches a system for controlling use of configuration data (abstract: write data, fig. 7: element 306: write data, col. 4 lines 18-21) comprising: a configurable device comprising: a sequence generator (col. 3 lines 1-3: "a secured corresponding copy of [the] message digest function generates a new digest," this reads on a sequence generator in the configurable device), and the configurable device further comprising: disabled user logic (col. 4 lines 28-30), a comparator configured to receive and compare a first sequence and a third sequence (col. 3 lines 8-16: the decrypted digest and the new digest generated in the configurable device are sent to a comparator, fig. 2 element 120: Comparison Function); and means connected to the comparator and the user logic for enabling the user logic if the first and third sequences are identical (col. 3 lines 8-16), and a decryptor configured to receive and decrypt a second sequence to generate a third sequence (fig. 2 element 116, col. 3 lines 3-6: The

configurable device decrypts the signed reference digest using a public key that corresponds to the private key: this reads on the generation of a third sequence). However, Albrecht does not teach a configurable device that generates a first sequence that it then sends to a secure device, whereupon the secure device encrypts it to produce a second sequence and returns the second sequence to the configurable device. However, Shona does teach these features (col. 5 lines 15-25). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features of Shona into the system of Albrecht. Motive to make this combination is found, for example in col. 1 lines 24-29 of Albrecht, where denial of unauthorized access to secure memory is discussed. Use of the terminal authentication challenge-response protocol of Shona would increase the difficulty of unauthorized access to secure memory.

As for claims 28 and 29, Albrecht teaches the system of Claim 17 wherein: the configurable device authorization code generator comprises a sequence generator in the configurable device configured to generate a first sequence as the configurable device authorization code (col. 3 lines 1-3); and the secure device authorization code generator comprises: an encryptor in the secure device (col. 2 lines 51-59), a decryptor (col. 3 lines 3-6) and a comparator (col. 3 lines 5-9: "comparison function"). However Albrecht does not further teach a sequence generator in the configurable device that is a pseudo-random number generator, or teach an encryptor in the secure device that is configured to receive and encrypt the first sequence to generate a second sequence

and wherein the configurable then receives and decrypts the second sequence from the secure device in order to generate a third sequence and to transmit the third sequence as the secure device authorization code to the comparator. However Shona does teach these features (col. 5 lines 15-25). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features of Shona into the system of Albrecht. Motive to make this combination is found, for example in col. 1 lines 24-29 of Albrecht, where denial of unauthorized access to secure memory is discussed. Use of the terminal authentication challenge-response protocol of Shona would increase the difficulty of unauthorized access to secure memory.

As for claim 30, the combination of Albrecht and Shona does not teach the use of an SRAM PLD. However Official Notice may be taken that the use of such memory in a PLD is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Albrecht. It would have been advantageous to do so since the use of such memory would eliminate the need for continual refreshes in order to keep the memory intact.

As for claim 31, the combination of Albrecht and Shona does not teach the use of an EEPROM PLD. However Official Notice may be taken that the use of such memory in a PLD is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this

feature into the system of Albrecht. It would have been advantageous to do so since the use of such memory would allow for rapid updating and long-term storage of the configuration data.

As for claims 49 and 50, they are directed towards the apparatus carrying out the method of claim 43. Therefore claims 49 and 50 are rejected on the same basis as is claim 43.

8. Claim 2-13, 19-22, 24-27, 34-37, 39-42, 44, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albrecht and Schrenk, US 5,889,266.

As for claims 2, 10, and 13, Albrecht teaches the method of claim 1 of generating a second sequence, and transmitting the second sequence to an encryptor in the secure device; encrypting the second sequence to generate a third sequence (col. 2 lines 60-67: The secure device calculates a reference digest of the write data, reading on generation of a first sequence, col. 2 lines 60-67: The secure device encrypts the reference digest under a private key to form a signed digest, reading on generation of a second sequence); transmitting the third sequence to a decryptor in the configurable device; and decrypting the third sequence to generate a fourth sequence (fig. 2 element 116, col. 3 lines 3-6: The configurable device decrypts the signed reference digest using a public key that corresponds to the private key). However Albrecht does not teach the additional steps where generating the configurable device authorization code comprises

generating a first sequence as the configurable device authorization code in a pseudo-random number generator in the configurable device; and generating the secure device authorization code comprises: generating a second sequence in a pseudo-random number generator in the secure device; and wherein the fourth sequence is the secure device authorization code. However, Schrenk does teach the use of such pseudorandom number generators to calculate a first sequence in a configurable device, and generation of an identical pseudorandom number in the secure device (col. 6 lines 64-67, col. 7 lines 1-14). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Albrecht. It would have been desirable to do so since this authentication of the terminal, in addition to authentication / authorization of the write data, would provide an additional layer of security on preventing unauthorized access to the configurable device memory.

As for claims 3, 7, 11, 20, 25, 35, 40, and 44, the combination of Albrecht and Schrenk does not teach the use of an SRAM PLD. However Official Notice may be taken that the use of such memory in a PLD is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Albrecht. It would have been advantageous to do so since the use of such memory would eliminate the need for continual refreshes in order to keep the memory intact.

As for claims 4, 8, 12, 21, 26, 36, 41, and 45, the combination of Albrecht and Schrenk does not teach the use of an EEPROM PLD. However Official Notice may be taken that the use of such memory in a PLD is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Albrecht. It would have been advantageous to do so since the use of such memory would allow for rapid updating and long-term storage of the configuration data.

As for claims 5, 24, and 42, Albrecht teaches the method of claims 2 and 17, but not the additional steps wherein the pseudo-random number generator in the secure device is a duplicate of the pseudo-random number generator in the configurable device and both pseudo-random number generators are seeded using the same seed. However, Schrenk does teach this feature (col. 6 lines 64-67, col. 7 lines 1-14). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Albrecht. It would have been desirable to do so since this seeding of identical pseudo-random number generators would allow authentication of the secure device (terminal), in addition to authentication / authorization of the write data, would provide an additional layer of security on preventing unauthorized access to the configurable device memory.

As for claims 6, 34, and 39, Albrecht teaches the method of claims 1, 33, 38 but not the additional steps wherein: generating the configurable device authorization code

comprises generating a first sequence as the configurable device authorization code in a pseudo-random number generator in the configurable device; and generating the secure device authorization code comprises generating a second sequence as the secure device authorization code in a pseudo-random number generator in the secure device. However, Schrenk does teach the use of such pseudorandom number generators to calculate a first sequence in a configurable device, and generation of an identical pseudorandom number in the secure device (col. 6 lines 64-67, col. 7 lines 1-14). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Albrecht. It would have been desirable to do so since this authentication of the terminal, in addition to authentication / authorization of the write data, would provide an additional layer of security on preventing unauthorized access to the configurable device memory.

As for claims 9, 19, 22, 27, and 37, Albrecht teaches the method of claims 6, 18, and 33, but not the additional steps wherein the pseudo-random number generator in the secure device is a duplicate of the pseudo-random number generator in the configurable device and both pseudo-random number generators are seeded using the same seed. However, Schrenk does teach the use of such identical pseudorandom number generators to calculate a first sequence in a configurable device, and generation of an identical pseudorandom number in the secure device (col. 6 lines 64-67, col. 7 lines 1-14). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Albrecht.

It would have been desirable to do so since this authentication of the terminal, in addition to authentication / authorization of the write data, would provide an additional layer of security on preventing unauthorized access to the configurable device memory.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent documents teach systems of authentication related to memory access and are pertinent to the applicants disclosure.

Leung	5,457,4008
Bahout	5,594,793
Sung et al.	5,768,372
Mattison	5,778,070
Curd et al.	5,838,901
Curd et al.	5,991,880
Davis	5,844,986
Brun et al.	6,662,283
Pang et al.	6,981,153

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

3-9-01

Paul Callahan

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER